COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

Annual Report

2003-2004

Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2004
ISBN 0-662-68250-5
Cat. No. D95-2004

Communications Security
Establishment Commissioner

The Right Honourable Antonio Lamer,
P.C., C.C., C.D., L.L.D., D.U.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

Le très honorable Antonio Lamer,
c.p., c.c., c.d., L.L.D., d.u.

June 2004

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to sub-section 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2003-2004 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Antonio Lamer

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

104-07751/

CONTENTS

Introduction 1

The Year in Review 2

- Governing authorities for foreign intelligence collection 3
- Ministerial authorizations 5
- Report of the Auditor General of Canada 7

2003-2004 Activities 8

- Reviews under the Commissioner's general mandate 8
- Reviews of activities under ministerial authorizations 8
- Review of past recommendations 9
- 2003-2004 Findings 10
- Complaints and concerns about CSE activities 10

The Commissioner's Office 11

- Office expenditures and staff 11

Looking Ahead 13

- New national security policy 13
- Proposed legislation 14
- Review agencies conference 16

Concluding Thoughts 16

Annex A: Mandate of the Communications Security Establishment Commissioner 17

Annex B: Statement of Expenditures 2003-2004 19

Annex C: Classified Reports, 1996-2004 21

INTRODUCTION

This is my first report as Communications Security Establishment (CSE) Commissioner following my appointment on June 19, 2003.

During my twenty years on the Supreme Court of Canada, ten of them as Chief Justice, I witnessed and participated in the evolution of human rights and freedoms in this country, as we grappled with the application and impact of the *Canadian Charter of Rights and Freedoms*. This experience dovetails very well with my duties as CSE Commissioner, because safeguarding the rights of Canadians, including in particular the right to privacy, is an important element, although not exhaustive, of my mandate. In accepting this order-in-council appointment last June, therefore, I was honoured and pleased to have the opportunity to continue serving my country in a meaningful way.

Since retiring from the Court, I have participated in independent reviews and inquiries. One lesson I took from those experiences was the value of working collaboratively when seeking change and reform. With this background, my approach to reviewing the activities of the Communications Security Establishment is essentially proactive and preventive. When reviewing CSE operations to ensure that no unlawful activity has occurred, I also look for the existence of preventive counter-measures to safeguard against situations arising in which unlawful activity *could* occur. In areas as vital as security and intelligence where Canadians' privacy is at stake, I believe this approach is not only warranted but essential in establishing the appropriate balance between the demands of security and intelligence and the privacy rights of Canadians.

Under this approach, if I had concerns as a result of a review conducted by my office, my first step would be to share those concerns with the relevant persons — the Chief of CSE and those who report

to him. This would afford them an opportunity to institute corrective measures or to explain to me why my concerns were unjustified. By proceeding in this way, it is my hope that when I submit classified reports to the Minister of National Defence, most of the problem areas I have identified will already have been addressed, and my report will have been rendered moot.

This approach has proved useful in the past, often resulting in prompt administrative action. As a result, it has been possible to improve the way things are done expeditiously and without confrontation. In this way, the review and reporting process becomes a vehicle not just for detecting unlawful activity but for preventing it in the first place. When constructive criticism is accepted in the spirit in which it is intended, this approach works to the benefit of all concerned.

THE YEAR IN REVIEW

To prepare myself for the work ahead, in the first few months after my appointment I received several briefings from my own staff and from officials at CSE, including meetings with the Chief and his executive team. I met with the Minister of National Defence as well as his predecessor. I also met with the Security Intelligence Review Committee and with the Security and Intelligence Coordinator, who is also the National Security Advisor to the Prime Minister, and to whom the Chief of CSE reports for matters of operations and policy.

What quickly became apparent to me was the array of challenges facing CSE and the rest of the intelligence community in light of globalized threats with implications for Canada's international affairs, defence and security. The need to monitor and understand these threats is vital, yet efforts to do so have been curtailed in recent years by what has become an increasingly complex web of global communication technologies. Significant

challenges to foreign intelligence collection — one of CSE's primary mandates — also arise in this environment.[1]

These and other new demands led to legislative amendments and the development of new legal frameworks that should meet two objectives: first, facilitating the activities of intelligence agencies; and second, requiring that those agencies meet certain standards and respect certain thresholds that allow them to define and account for their activities.

In parallel with technological development to permit foreign intelligence collection in an ever expanding and complex global communications environment, it is also important to develop technologies that enable intelligence agencies to protect the rights and privacy of Canadians. In other words, technology developed for purposes of acquiring information from the global information infrastructure *must* be complemented by technology that can be used to protect privacy. It is in this context that the need for review of CSE's activities remains high.

Against this backdrop, several general issues related to foreign intelligence collection drew my attention in the past year; two in particular warrant discussion here.

Governing authorities for foreign intelligence collection

Canada's intelligence requirements, including its foreign intelligence priorities, are established annually by the Ad Hoc Committee on Intelligence Priorities (formerly the Meeting of Ministers on Security and Intelligence), chaired by the Prime Minister. Several federal agencies, including the Communications Security Establishment, contribute to meeting these priorities.

[1] *Foreign intelligence* is defined in the *National Defence Act* as information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security (Part V.1, section 273.61).

To carry out its foreign intelligence mandate, the CSE relies on the authority of the *National Defence Act (NDA)*,[2] which empowers CSE to "acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities". When CSE does this, it is acting as a *principal* provider of foreign intelligence.

In addition, CSE, under the authority of the *NDA*, assists other federal agencies in the performance of their lawful duties. In these instances, CSE does so as an *agent*. In providing technical and operational assistance to federal law enforcement and security agencies, CSE is strictly governed by the terms and conditions of the principal's governing authorities, which in some instances may be a warrant from the Federal Court of Canada.

These two roles — as principal and agent — were formalized in legislation in 2001, but they are not new for CSE. What is new is CSE's authority under the *NDA* to intercept private communications, under prescribed conditions, if authorized to do so by the Minister of National Defence.[3] With a ministerial authorization, CSE can intercept and use a communication with a connection to Canada (that is, a 'private communication') acquired in the course of targeting a foreign entity abroad, provided it meets certain conditions laid out in the

---

[2] R.S.C. 1985, c. N-5.

[3] *Private communications* are the communications of Canadians or persons in Canada. Specifically, *private communication* is defined in section 183 of the *Criminal Code* as any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.

NDA. This provision adds a new authority to the legal framework within which foreign intelligence can be lawfully acquired.

From my initial review of some foreign intelligence collection activities, I had concerns that, in some instances, the linkages between these activities and the authorities that govern them were not being given due consideration. I was pleased to learn, therefore, that during the past year the legal frameworks available to the intelligence community for foreign intelligence collection were revisited to ensure that all available authorities had been fully considered before foreign intelligence activities were authorized. I encourage the government to continue to do so.

Ministerial authorizations

Historically, governments have relied on intelligence gathering as part of their efforts to protect and promote national interests and to identify and counter threats to those interests. The advent of new technologies, along with revolutionary developments in the communications industry over the past decade, have hindered some traditional forms of intelligence collection, including the foreign signals intelligence collection performed by CSE.

In the not so distant past, foreign intelligence collection was fashioned around predictable communications patterns and technologies. As a result, it could be conducted within relatively neatly defined legal frameworks. This environment facilitated the review and assessment of foreign intelligence collection activities. During my first year as CSE Commissioner, however, I quickly understood that this is no longer the case. Governments have had to reassess their ability to protect national interests and counter activities such as terrorism that threaten domestic and international security. Canada is no exception.

New legal mechanisms were needed to respond to this changing environment. One response was the ministerial authorization (MA) provisions in Part V.1 of the *National Defence Act*, added to the Act in 2001.[4]

Today's integrated technologies carry different kinds of traffic and follow complex communication paths that transit international borders and mix foreign communications with private communications. The MA provisions do not allow CSE to target Canadians or their communications. (CSE has never been allowed to do this.) Today, however, CSE is in a better position to fulfil its foreign intelligence responsibilities because, with the Minister's consent, it can follow targeted foreign communications even if they have a connection with Canada. I believe that few Canadians would disagree with the intent of this provision and the authority it provides in today's context of terrorism and threats to Canadians' safety and security.

Since the new legislation was passed, I can confirm that CSE has exercised this authority. As CSE Commissioner, I understand the need for it and support its objective. Subsection 273.65 (8) of the *NDA* requires that I review CSE activities carried out under an MA to ensure that they are authorized and report annually to the Minister.

---

[4] Part V.1 was added to the *National Defence Act* by the *Anti-Terrorism Act*, which became law on December 24, 2001. Before issuing a ministerial authorization, the Minister must be satisfied that the four conditions set out in subsection 273.65 (2) of the *NDA* have been met:

(a) the interception will be directed at foreign entities located outside Canada;

(b) the information to be obtained could not reasonably be obtained by other means;

(c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and

(d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

I believe CSE's policies, instruments and processes must require and facilitate the management and accountability of any activities it conducts under the authority of an MA, particularly activities that relate to intercepting private communications and safeguarding the privacy of Canadians. While this is an evolving process, I can report that CSE has continued to improve the MA structure and strengthened the MA management and accountability mechanisms.

Report of the Auditor General of Canada

The Auditor General's November 2003 report was tabled in Parliament on February 11, 2004. Chapter 10 of the report — Other Audit Observations — included an audit note, headed *Independent reviews of security and intelligence agencies*, that went on to state, "The activities of security and intelligence agencies are not subject to consistent levels of review and disclosure."

The report suggested that the CSE Commissioner's annual report should be expanded beyond considering CSE's compliance with the law to include such topics as management issues or potential problems at CSE. I believe that a review of the annual reports produced by this office to date will confirm that these areas have, in fact, been considered as they relate to two of the organization's business lines, foreign intelligence collection and the protection of government information systems and networks.

For example, over the past several years, reviews have led to observations in such areas as CSE's strategic planning activities; internal policies, procedures and handling practices; and management and control frameworks. These observations have always been made, however, in the context of lawfulness and CSE's efforts to safeguard the privacy of Canadians.

I believe the content of the CSE Commissioner's public annual report must be guided by his mandate, which is to review and report on CSE's activities to ensure that they are in compliance with the law, and to report to the Minister of National Defence annually on the Commissioner's activities and findings.

2003-2004 ACTIVITIES

I submitted a total of five classified reports to the Minister of National Defence over the period covered by this report. Two of these were initiated by my predecessor and completed during the first year of my term.

Reviews under the Commissioner's general mandate

In 2003-2004, I submitted three classified reports to the Minister of National Defence on subjects related to my general mandate to review CSE's activities to ensure they conform with the law.

Submitting a classified report to the Minister does not mean that a lack of compliance with the law or ministerial authority has been detected. It indicates only that the report contains material that requires classified handling. I report to the Minister on all my reviews, either to provide assurance or to bring concerns to his attention, as each specific situation requires.

Reviews of activities under ministerial authorizations

CSE conducted activities under seven ministerial authorizations in 2002-2003; two of these concerned foreign intelligence collection, while five related to information technology security. Within the time frame covered by this report, my office reviewed activities under five of the MAs; the others were nearing completion at the end of the reporting year. The five reviews resulted in two reports to the Minister, both covering information technology security activities.

None of the reports raised issues of unlawfulness.

However, a more general issue about the structure of and process for using ministerial authorizations did arise. Certain weaknesses in policies and procedures related to these activities were brought to CSE's attention. While some issues have been resolved, others remain. I hope to be able to report further on these issues in next year's report.

Annex C provides a list of all classified reports to the Minister submitted by my predecessor and me since the Commissioner's office was established in 1996.

Review of past recommendations

This year my staff reviewed all recommendations made by my predecessor and me in classified reports submitted to the Minister of National Defence since the creation of this office in 1996. The goal was to follow up with CSE on these recommendations and to determine whether the issues identified had been dealt with satisfactorily. I will be asking CSE for an annual update of this information.

The review showed that CSE's response to the recommendations has not been uniform. This is not surprising, given the diverse nature of the recommendations made to date: some could be implemented immediately; some related to policy or procedures; some were of a technical nature; and some required further study to determine their feasibility. Many related to how CSE can better manage and account for its activities.

Based on this review, I would observe that CSE has responded to many of the Commissioner's recommendations, but that a number of issues remain to be addressed, in particular, by establishing work plans and timetables with milestones and completion dates for specific corrective actions that CSE has acknowledged are necessary.

As I have made clear throughout this report, my recommendations and those of my predecessor are intended generally to be preventive, to forestall the

possibility of non-compliance by putting effective controls in place. It is in this spirit that I will continue to follow up on CSE's response to recommendations from my office.

2003-2004 Findings

I can report that the activities of CSE that my office reviewed during the past year complied with the law and with ministerial authority. It is important to place this assertion in context. It should not be taken to mean that I am certifying that all CSE's activities in 2003-2004 were lawful. I cannot make this assertion, because I did not review all their activities — and no independent reviewer could. However, my office reviews a wide range of activities in considerable depth, based on our assessment of where the risks of unlawful activity are likely to be greatest. This is the appropriate context for the assurance my work provides.

I should add, however, that during the course of reviews, I occasionally identify circumstances where there are clear and evident risks that unlawful activity might occur (arising, for example, from deficiencies in policies or practices). My predecessor and I have made a practice of reporting these circumstances to CSE and to the Minister. As I made clear in the introduction to this report, I believe it is ultimately more useful to prevent unlawful activity than to identify it after the fact.

Complaints and concerns about CSE activities

There were two complaints in the period covered by this report, but neither led to a formal investigation.

If I am to be in a position to assure complainants that CSE is not engaging in unlawful activity, my approach to complaints must take into account the mandate assigned to CSE under Part V.1 of the *National Defence Act*. Now, as before the introduction of Part V.1, CSE must not target

the communications of Canadians or persons in Canada. As discussed earlier, however, it is no longer possible to state unequivocally that both ends of a communication intercepted by CSE are foreign. CSE can now intercept (though it cannot target) private communications, provided it obtains a ministerial authorization in advance. CSE may also use and retain that communication, provided it adheres to guidelines that are also established in Part V.1 of the *NDA* (see footnote 4).

Any complaint submitted to me about CSE's activities must therefore be examined in this light.

No persons approached me to avail themselves of the public interest defence provisions of the *Security of Information Act*, subparagraph 15 (5)(b)(ii).[5]

THE COMMISSIONER'S OFFICE

Office expenditures and staff

Since 1996, when the position was first created, the mandate of the Communications Security Establishment Commissioner — and hence the staff and other resources required to carry out that mandate — have undergone considerable evolution. Between June 1996 and December 2001, the Commissioner's role was twofold: to review CSE's activities to determine whether they conformed with the law, and to receive complaints about the lawfulness of CSE activities.

As discussed at length in previous annual reports and alluded to earlier in this report, two features of the *Anti-Terrorism Act* of December 2001 had a direct bearing on the Commissioner's functions: the review of CSE activities conducted under ministerial authorization and the Commissioner's duties under the *Security of Information Act*.

---

[5] R.S.C. 1985, c. O-5.

To fulfil these new responsibilities, my office was allocated additional resources to carry out review activities. A bigger workload and more staff have affected the way we organize and manage our work. For example, our internal policies and procedures for managing the office have been enhanced to reflect the maturation of the organization and the increase in staff during the fiscal year.

We have also paid attention to our work methods. Tools such as a standardized methodology, scope statements, and guidelines structure our reviews of CSE's activities in such a way that all reviewers are working to the same standards of rigour and thoroughness. With the addition of more staff involved in these endeavours, my office has embarked on an initiative to record and document these processes wherever possible.

With a new Commissioner and the evolution of the Commissioner's mandate over the past three years, it was time to look at how my office relates to the broader context in which it operates — in particular the federal government community and the security and intelligence community in Canada and internationally. A communications plan, developed this year with input from key players in Canadian intelligence, will help guide my office through the rapidly evolving intelligence and policy worlds.

For example, one objective of the plan is to communicate more regularly and systematically with interested groups and individuals — including the Canadian intelligence community, organizations that deal with intelligence issues, and academics specializing in the intelligence field — about the nature of my mandate, my approach to the job, and the activities of my office. This type of interaction could lead, for instance, to productive partnerships with academic specialists in areas of mutual interest and concern. In addition, conveying accurate,

timely information about the office will help avoid misunderstandings or speculation about who we are and what we do.

Among the first steps in implementing the plan were my meetings with the current and former Ministers of National Defence, the chair and members of the Security Intelligence Review Committee, and the National Security Adviser to the Prime Minister, mentioned earlier.

In addition, my staff met with academics specialized in security and intelligence matters and participated in meetings of the Canadian Association of Security and Intelligence Studies. My staff also took steps toward greater participation in the public service community — notably through meetings with other small agencies, particularly those whose mandates include reviews and complaints.

With regard to the broader security and intelligence community, my office received visiting parliamentarians from Sweden and the United Kingdom — both countries with similar concerns but different review models from Canada's. In the past the office would not have had sufficient staff resources to undertake this range of activities, but the hiring of a director of review and government liaison and a director of review and military liaison will permit continued involvement in these communities in the future.

LOOKING AHEAD

New national security policy

On April 27, 2004, the government tabled in Parliament its first national security policy, entitled *Securing an Open Society: Canada's National Security Policy*. The policy addresses a range of national security issues and provides guidance in six strategic areas: intelligence, emergency planning and management, public health, transport security, border security, and international security.

The policy also calls for the development of new structures and strategies that the government believes will enable it to anticipate and manage current and future threats to Canada's national security interests.

Among the changes in government structure announced on December 12, 2003, and confirmed in the national security policy announcement, was a proposal to establish a new committee of parliamentarians whose members would be sworn in as Privy Councillors so they could be briefed on national security issues.

These initiatives obviously have the potential to influence the activities of my office, but it is too early to say what the shape or extent of this influence might be. My staff and I will be following developments closely with a view to providing input where appropriate.

Proposed legislation

Two legislative proposals before Parliament at the end of this reporting year may have additional implications for my office:

- Passage of Bill C-7 (formerly Bill C-17), the Public Safety Act, 2002, would entail new responsibilities for the Commissioner. The bill amends the *National Defence Act* to confer significant new responsibilities on the Commissioner of CSE for reviewing the lawfulness of activities undertaken by the Department of National Defence and the Canadian Forces to maintain and protect their computer systems and networks and for dealing with complaints arising from such activities.[6]

---

[6] Bill C-7, An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order t enhance public safety, 3rd Sess., 37th Parl., 2004; Bill C-17, An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety, 2nd Sess., 37th Parl., 2002.

- Bill C-14 (formerly Bill C-32) amends provisions of the *Criminal Code* and the *Financial Administration Act*, among other acts. It introduces new provisions, including a new authority to intercept private communications for the purpose of managing and protecting computer systems and networks. There is a question of how this bill will affect the provisions and passage of the proposed Public Safety Act, 2002, which has similar wording.[7]

My concerns are threefold:

- the fact that passage of both bills would establish different governing authorities dealing with essentially similar activities;
- the fact that passage of Bill C-7 would impose on the Department of National Defence a different accountability regime than would be imposed on other departments by passage of Bill C-14; and
- the difficulties I am likely to encounter in providing meaningful assurance of lawfulness and compliance with ministerial authority as envisaged in Bill C-7.

Developments in two other areas may also have implications for my office:

- Parliament's statutory review of the *Anti-Terrorism Act* three years after its initial passage into law is slated to begin by the end of 2004. I intend to provide my comments based on my observations to date.
- The government introduced Bill C-25, the so-called whistle-blower legislation, on

[7] Bill C-14, An Act to amend the *Criminal Code* and other Acts, 3rd Sess., 37th Parl., 2004; Bill C-32, An Act to amend the *Criminal Code* and other Acts, 2nd Sess., 37th Parl., 2003.

March 22, 2004.[8] Although CSE would be exempt from this legislation, it would have to establish a system to serve essentially the same purpose, raising questions about a possible role for the Commissioner.

We will be following these and other developments closely to determine their likely impact on this office, as well as where and how we can contribute our input most effectively.

Review agencies conference

The next International Intelligence Review Agencies Conference will be held in Washington, D.C., in October 2004. Representatives of review agencies from Australia, Canada, New Zealand, the United States, the United Kingdom and other countries will meet to exchange views on issues of common interest. I look forward to receiving this year's agenda.

CONCLUDING THOUGHTS

Looking back over the year, I would like to thank my predecessor as Commissioner, the Honourable Claude Bisson, O.C., who laid a strong foundation for the Office of the CSE Commissioner and from whom I inherited a superb staff and an organization well positioned to meet the challenges ahead. Thanks to this legacy, the transition between our tenures was smooth, and I was able to assume my responsibilities quickly and efficiently.

Based on my experience over the past nine months, I believe that my mandate and resources as Commissioner are adequate to discharge my legislated duties. I look forward to continuing the productive relationship established with the Minister, with CSE and with other government officials as we fulfil our respective roles in Canada's security and intelligence community.

---

[8] An Act to establish a procedure for the disclosure of wrongdoings in the public sector, including the protection of persons who disclose the wrongdoings. Its short title would be the Public Servants Disclosure Protection Act, 3rd Sess., 37th Parl., 2004.

Mandate of the Communications Security Establishment Commissioner

National Defence Act – Part V.1

"**273.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

"**273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review."

Security of Information Act

"**15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest.

"**15.** (5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following:

"**15.** (5) (b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to,

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time."

Statement of Expenditures 2003-2004

Standard Object Summary

Salaries and Wages	352,505
Transportation and Telecommunications	22,227
Information	43,201
Professional and Special Services	246,323
Rentals	134,794
Purchased Repair and Maintenance	42,019
Materials and Supplies	9,708
Acquisition of Machinery and Equipment	51,451
Other Expenditures	104
Total	**$902,332**

Classified Reports, 1996-2004

Classified Report to the Minister – March 3, 1997 (TOP SECRET)

Classified Report to the Minister
- Operational Policies with Lawfulness Implications - February 6, 1998 - (SECRET)

Classified Report to the Minister
- CSE's Activities under *** - March 5, 1998 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
- Internal Investigations and Complaints - March 10, 1998 (SECRET)

Classified Report to the Minister
- CSE's activities under *** - December 10, 1998 (TOP SECRET/CEO)

Classified Report to the Minister
- On controlling communications security (COMSEC) material - May 6, 1999 (TOP SECRET)

Classified Report to the Minister
- How We Test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) - June 14, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
- A Study of the *** Collection Program - November 19, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
- On *** - December 8, 1999 (TOP SECRET - COMINT)

Classified Report to the Minister
- A Study of the *** Reporting Process - an overview (Phase I) - December 8, 1999 (SECRET/CEO)

Classified Report to the Minister
- A Study of Selection and *** - an overview - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's Operational Support Activities Under *** - follow-up - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - May 10, 2000 (SECRET)

Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - June 15, 2000 (SECRET)

Classified Report to the Minister
- CSE's Policy System Review - September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase II *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase III *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister
- CSE's participation *** - August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's support to *** as authorized by *** and *** - August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister
- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) - August 21, 2002 (SECRET)

Classified Report to the Minister
- CSE's support to XXX, as authorized by *** and code named *** - November 13, 2002 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's SIGINT activities carried out under the *** 2002 *** ministerial authorization November 27, 2002 (TOP SECRET/CEO)

Classified Report to the Minister
- Lexicon - 26 March 2003 (TOP SECRET/COMINT)

Classified Report to the Minister
- CSE's activities pursuant to three XXX ministerial authorizations including *** *** - May 20, 2003 (SECRET)

Classified Report to the Minister
- CSE's support to XXX, as authorized by *** and code named *** - Part I - November 6, 2003 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister
- CSE's support to XXX, as authorized by *** and code named *** - Part II - March 15, 2004 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister
- A review of CSE's activities conducted under XXX ministerial authorization - March 19, 2004 (SECRET/CEO)

Classified Report to the Minister
- Internal investigations and complaints - Follow-up - March 25, 2004 (TOP SECRET/CEO)

Commissaire
du Centre
de la sécurité
des télécommunications

Rapport annuel

2003-2004

Canada

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096

© Ministre des Travaux publics et des Services gouvernementaux Canada 2004
ISBN 0-662-68250-5
N° de cat. D95-2004

Commissaire du Centre de la
sécurité des télécommunications

Le très honorable Antonio Lamer,
c.p., c.c., c.d., L.L.D., d.u.

CANADA

Communications Security
Establishment Commissioner

The Right Honourable Antonio Lamer,
P.C., C.C., C.D., L.L.D., D.U.

Juin 2004

Ministre de la Défense nationale
Édifice Mgén G.R. Pearkes, 13e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63 (3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 2003-2004, qui fait état de mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Antonio Lamer

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE DES MATIÈRES

Introduction 1

Rétrospective de l'année 2
- Autorisations régissant la collecte de renseignements étrangers 4
- Autorisations ministérielles 5
- Rapport de la vérificatrice générale du Canada 8

Activités de l'année 2003-2004 9
- Examens relevant du mandat général du commissaire 9
- Examens d'activités entreprises en vertu d'autorisations ministérielles 9
- Examen des recommandations antérieures 10
- Constatations faites en 2003-2004 11
- Plaintes et préoccupations au sujet des activités du CST 11

Le bureau du commissaire 12
- Dépenses du bureau et personnel 12

Coup d'œil sur l'avenir 15
- La nouvelle politique de sécurité nationale 15
- Mesures législatives proposées 16
- Conférence des organismes d'examen 18

Conclusion 18

Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications 19

Annexe B : État des dépenses, 2003-2004 21

Annexe C : Rapports classifiés de 1996 à 2004 23

INTRODUCTION

Ce rapport est le premier que je présente à titre de commissaire du Centre de la sécurité des télécommunications (CST) depuis ma nomination, le 19 juin 2003.

Au cours des vingt années pendant lesquelles j'ai siégé à la Cour suprême du Canada, dont dix à titre de juge en chef, j'ai participé à l'évolution des droits et libertés de la personne dans notre pays, à la fois comme témoin et comme acteur, dans le cadre de nos débats touchant l'application et l'incidence de la *Charte canadienne des droits et libertés*. Cette expérience cadre très bien avec mes fonctions de commissaire du CST, car la sauvegarde des droits des Canadiens, notamment le droit à la vie privée, constitue un élément important, quoique non exhaustif, de mon mandat. Lorsque j'ai accepté cette nomination par décret, en juin dernier, j'ai donc été honoré et heureux d'avoir l'occasion de continuer à servir utilement mon pays.

Depuis ma retraite de la Cour, j'ai participé à des enquêtes et à des examens indépendants. L'un des enseignements que j'ai tirés de ces expériences a été la valeur du travail en collaboration lorsque l'on cherche à effectuer des changements et des réformes. Ces antécédents font que mon approche de l'examen des activités du Centre de la sécurité des télécommunications est essentiellement prévisionnelle et préventive. Ainsi, lorsque j'examine les opérations du CST pour m'assurer qu'on ne s'y est livré à aucune activité illégale, je cherche en outre s'il existe des contre-mesures préventives permettant d'éviter les situations où des activités illégales *pourraient* se produire. J'estime que, dans des domaines aussi fondamentaux que la sécurité et le renseignement, où la vie privée des Canadiens est en jeu, cette approche est non seulement justifiée mais essentielle pour établir l'équilibre approprié entre les exigences de la sécurité et du renseignement et les droits à la vie privée des Canadiens.

Selon cette approche, si j'avais des inquiétudes par suite d'un examen effectué par mon bureau, ma première démarche consisterait à en faire part aux personnes compétentes, soit le chef du CST et ses subordonnés. Cela leur fournirait l'occasion de prendre des mesures correctives ou de m'expliquer pourquoi mes inquiétudes sont injustifiées. J'espère que, en procédant de cette manière, la plupart des problèmes que j'aurai détectés auront déjà été résolus au moment où je présenterai des rapports classifiés au ministre de la Défense nationale, de sorte que ceux-ci auront alors perdu leur intérêt pratique.

Cette approche s'est révélée fructueuse par le passé et elle a souvent suscité des mesures administratives rapides. En conséquence, il a été possible d'améliorer la façon de faire les choses promptement et sans conflit. De cette manière, le processus d'examen et de rapport devient un moyen non seulement de déceler les activités illégales, mais de les prévenir. Lorsque les critiques constructives sont acceptées dans l'esprit où elles sont faites, cette approche avantage toutes les parties intéressées.

RÉTROSPECTIVE DE L'ANNÉE

Au cours des premiers mois qui ont suivi ma nomination, j'ai reçu plusieurs séances d'information de mon propre personnel et des fonctionnaires du CST, y compris des réunions avec le chef et son équipe exécutive, en vue de me préparer au travail que j'allais devoir faire. J'ai rencontré le ministre de la Défense nationale actuel, ainsi que son prédécesseur. J'ai également rencontré le Comité de surveillance des activités de renseignement de sécurité et le coordonnateur de la sécurité et du renseignement, qui fait en outre fonction de conseiller en matière de sécurité nationale auprès du Premier ministre et de qui relève le chef du CST pour les questions d'opérations et de politique.

J'ai vite pris conscience de l'ensemble des défis auxquels sont confrontés le CST et le reste de la collectivité du renseignement compte tenu des menaces mondialisées qui ont des incidences sur les affaires internationales, sur la défense et sur la sécurité du Canada. Il est capital de surveiller ces menaces et de les comprendre; néanmoins, les efforts déployés dans ce sens ont été restreints ces dernières années par ce qui est devenu un réseau de plus en plus complexe de technologies de communication mondiale. Ce contexte présente en outre des défis importants pour ce qui est de la collecte de renseignements étrangers, qui constitue l'un des principaux mandats du CST[1].

Ces défis et d'autres exigences nouvelles ont entraîné des modifications législatives et l'élaboration de nouveaux cadres juridiques qui devraient favoriser l'atteinte de deux objectifs, soit faciliter les activités des organismes de renseignement, et exiger que ceux-ci satisfassent à certaines normes et respectent certains seuils qui leur permettent de définir leurs activités et d'en rendre compte.

Parallèlement à l'évolution technologique visant à permettre la collecte de renseignements étrangers dans un contexte de communications mondiales de plus en plus large et complexe, il importe de mettre au point des technologies grâce auxquelles les organismes de renseignement pourront protéger les droits et la vie privée des Canadiens. Autrement dit, la technologie créée dans le but de tirer des renseignements de l'infrastructure mondiale d'information *doit* être complétée par une technologie pouvant être utilisée pour protéger la vie privée. C'est dans ce contexte que le besoin d'examen des activités du CST reste important.

---

[1] La *Loi sur la défense nationale* définit les *renseignements étrangers* comme suit : renseignements sur les moyens, les intentions ou les activités d'un étranger, d'un État étranger, d'une organisation étrangère ou d'un groupe terroriste étranger et qui portent sur les affaires internationales, la défense ou la sécurité (partie V.1, article 273.61).

À la lumière de ces faits, plusieurs questions générales liées à la collecte de renseignements étrangers ont attiré mon attention au cours de la dernière année; deux d'entre elles méritent d'être examinées ici.

Autorisations régissant la collecte de renseignements étrangers

Les besoins de renseignement du Canada, y compris ses priorités en matière de renseignements étrangers, sont établis annuellement par le Comité spécial sur les priorités en matière de renseignement (auparavant la Réunion des ministres sur la sécurité et le renseignement), que préside le Premier ministre. Plusieurs organismes fédéraux, dont le Centre de la sécurité des télécommunications, contribuent à répondre à ces priorités.

Pour remplir son mandat en matière de renseignements étrangers, le CST s'appuie sur la *Loi sur la défense nationale (LDN*[2]*)*, qui l'habilite à « acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement ». Lorsqu'il fait cela, le CST agit à titre de fournisseur *principal* de renseignements étrangers.

En vertu de la *LDN*, le CST aide en outre d'autres organismes fédéraux à remplir les fonctions que leur confère la loi. Dans ces cas, il fait fonction d'*agent*. Lorsqu'il apporte une aide technique et opérationnelle aux organismes fédéraux d'exécution de la loi et de sécurité, le CST est régi strictement par les modalités des autorisations régissant l'organisme principal, qui, dans certains cas, peuvent être un mandat de la Cour fédérale du Canada.

Ces deux rôles — celui de fournisseur principal et celui d'agent — ont été officialisés dans la loi en 2001, mais ils ne sont pas nouveaux pour le CST.

[2] L.R.C. (1985), chap. N-5.

Ce qui est nouveau, c'est le pouvoir que lui confère la *LDN* d'intercepter des communications privées, dans des conditions prescrites, s'il est autorisé à cette fin par le ministre de la Défense nationale[3]. Lorsqu'il possède une autorisation ministérielle, le CST peut intercepter et utiliser une communication ayant un rapport avec le Canada (c'est-à-dire une « communication privée ») acquise à l'occasion du ciblage d'une entité étrangère à l'étranger, pourvu qu'il satisfasse à certaines conditions énoncées dans la *LDN*. Cette disposition ajoute un nouveau pouvoir au cadre juridique à l'intérieur duquel les renseignements étrangers peuvent être acquis légalement.

À la suite de mon examen initial de certaines activités de collecte de renseignements étrangers, je me suis inquiété de ce que, dans certains cas, l'on ne tenait pas dûment compte des liens entre ces activités et les autorisations qui les régissent. J'ai donc été heureux d'apprendre que, au cours de la dernière année, on avait réexaminé les cadres juridiques mis à la disposition de la collectivité du renseignement aux fins de la collecte de renseignements étrangers, afin d'assurer que l'on avait pleinement tenu compte de toutes les autorisations disponibles avant d'autoriser les activités de renseignements étrangers. J'encourage le gouvernement à continuer d'agir dans ce sens.

Autorisations ministérielles

Par le passé, les gouvernements comptaient sur la collecte de renseignements dans le cadre de leurs efforts en vue de protéger et promouvoir les intérêts

[3] Les *communications privées* sont les communications de Canadiens ou de personnes se trouvant au Canada. Plus précisément, l'article 183 du *Code criminel* définit une *communication privée* comme suit : communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.

nationaux et de déceler et contrer les menaces planant sur ceux-ci. L'avènement de technologies nouvelles ainsi que les progrès révolutionnaires accomplis dans l'industrie des communications au cours de la dernière décennie ont entravé certaines formes traditionnelles de collecte de renseignements, dont celle du renseignement électromagnétique étranger effectuée par le CST.

Il n'y a pas si longtemps, la collecte de renseignements étrangers s'articulait autour de modes et de technologies de communication prévisibles. Elle pouvait par conséquent être effectuée à l'intérieur de cadres juridiques relativement bien définis. Ce contexte facilitait l'examen et l'évaluation des activités de collecte de ces renseignements. Au cours de la première année de mon mandat de commissaire du CST, toutefois, j'ai vite compris que ce n'est plus le cas. Les gouvernements ont dû réévaluer leur capacité de protéger les intérêts nationaux et de contrer des activités comme le terrorisme, qui menacent la sécurité nationale et internationale. Le Canada ne fait pas exception à cet égard.

De nouveaux mécanismes juridiques étaient nécessaires pour tenir compte de ce contexte en mutation. Les dispositions relatives à l'autorisation ministérielle (AM), ajoutées à la partie V.1 de la *Loi sur la défense nationale* en 2001, ont constitué l'une de ces réponses[4].

---

[4] La partie V.1 a été ajoutée à la *Loi sur la défense nationale* par la *Loi antiterroriste*, qui est entrée en vigueur le 24 décembre 2001. Avant de donner une autorisation, le ministre doit être convaincu que les quatre conditions énoncées au paragraphe 273.65(2) de la *LDN* sont remplies, soit :

a) l'interception vise des entités étrangères situées à l'extérieur du Canada;
b) les renseignements à obtenir ne peuvent raisonnablement être obtenus d'une autre manière;
c) la valeur des renseignements étrangers que l'on espère obtenir grâce à l'interception justifie l'interception envisagée;
d) il existe des mesures satisfaisantes pour protéger la vie privée des Canadiens et pour faire en sorte que les communications privées ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité.

Les technologies intégrées d'aujourd'hui écoulent différents genres de trafic et suivent des voies de communication complexes qui traversent les frontières internationales et mêlent les communications étrangères avec les communications privées. Les dispositions relatives à l'AM ne permettent pas au CST de cibler les Canadiens ni leurs communications. (Le CST n'a jamais été autorisé à faire cela.) Aujourd'hui, le CST est cependant mieux à même de s'acquitter de ses responsabilités en matière de renseignement étranger parce qu'il peut, avec le consentement du ministre, cibler les communications étrangères même si elles ont un lien avec le Canada. Je pense que peu de Canadiens se trouveraient en désaccord avec l'objet de cette disposition et le pouvoir qu'elle donne dans le contexte actuel de terrorisme et de menaces pour la sûreté et la sécurité des Canadiens.

Je suis à même d'affirmer que, depuis l'adoption de cette nouvelle mesure législative, le CST a exercé ce pouvoir. À titre de commissaire du CST, j'en comprends le besoin et j'en appuie l'objectif. Le paragraphe 273.65(8) de la *LDN* m'oblige à examiner les activités exercées par le CST en vertu d'une AM pour m'assurer qu'elles sont autorisées, et à faire rapport annuellement au ministre.

Je pense que les politiques, instruments et processus du CST doivent exiger et faciliter la gestion et la responsabilisation de toutes les activités qu'il exerce en vertu d'une AM, en particulier celles qui ont trait à l'interception de communications privées et à la sauvegarde de la vie privée des Canadiens. Bien que ce processus évolue, je peux déclarer que le CST a continué d'améliorer la structure de l'AM et en a renforcé les mécanismes de gestion et de responsabilisation.

Rapport de la vérificatrice générale du Canada

Le rapport de la vérificatrice générale daté de novembre 2003 a été déposé au Parlement le 11 février 2004. Le chapitre 10 de ce rapport — Autres observations de vérification — comprenait une note de vérification intitulée *Les activités de surveillance indépendante visant les organismes de sécurité et de renseignement*, qui disait ceci : « Il y a manque de cohérence quant au degré de surveillance et aux obligations de divulgation auxquels les organismes de sécurité et de renseignement sont soumis. »

La vérificatrice générale donnait à entendre que le rapport annuel du commissaire du CST devrait traiter, en plus de la conformité du CST à la loi, de sujets comme les questions de gestion ou les problèmes potentiels au CST. Je pense qu'un examen des rapports annuels publiés par mon bureau jusqu'ici révélera que ces sujets ont effectivement été abordés, car ils ont trait à deux des secteurs d'activité de l'organisme, soit la collecte de renseignements étrangers et la protection des systèmes et réseaux d'information du gouvernement.

Par exemple, ces dernières années, les examens ont mené à la formulation d'observations dans des domaines comme les activités de planification stratégique du CST, ses politiques, procédures et pratiques internes, et les cadres de gestion et de contrôle. Ces observations ont cependant toujours été faites dans le contexte de la légalité et des efforts déployés par le CST pour sauvegarder la vie privée des Canadiens.

Je pense que la teneur du rapport annuel public du commissaire du CST doit être déterminée par son mandat, qui est d'examiner les activités du CST et d'en faire rapport du point de vue de leur conformité à la loi, et de faire rapport annuellement au ministre de la Défense nationale de ses propres activités et de ses constatations.

ACTIVITÉS DE L'ANNÉE 2003-2004

J'ai adressé cinq rapports classifiés au ministre de la Défense nationale au cours de la période couverte par le présent rapport. Deux de ceux-ci avaient été entrepris par mon prédécesseur et ont été achevés pendant la première année de mon mandat.

Examens relevant du mandat général du commissaire

En 2003-2004, j'ai présenté au ministre de la Défense nationale trois rapports classifiés portant sur des sujets liés à mon mandat général d'examiner les activités du CST pour assurer leur conformité à la loi.

La présentation d'un rapport classifié au ministre ne signifie pas qu'un défaut de conformité à la loi ou à l'autorisation ministérielle a été détecté. Elle indique seulement que le rapport contient des éléments qui exigent une classification. Je fais rapport au ministre de tous mes examens, soit pour le rassurer, soit pour lui signaler des préoccupations, selon ce que la situation exige.

Examens d'activités entreprises en vertu d'autorisations ministérielles

Le CST a entrepris des activités en vertu de sept autorisations ministérielles en 2002-2003; sur celles-ci, deux concernaient la collecte de renseignements étrangers et cinq avaient trait à la sécurité des technologies de l'information. Au cours de la période couverte par le présent rapport, mon bureau a examiné les activités menées en vertu de cinq des AM; l'examen des autres activités était presque terminé à la fin de l'année faisant l'objet du rapport. Les cinq examens ont débouché sur la présentation de deux rapports au ministre, portant tous les deux sur les activités relatives à la sécurité des technologies de l'information.

Aucun de ces rapports n'a soulevé de questions d'illégalité. Toutefois, une question plus générale au sujet de la structure des autorisations ministérielles et de leur processus d'utilisation s'est posée.

Certaines faiblesses inhérentes aux politiques et aux procédures relatives à ces activités ont été portées à l'attention du CST. Certaines questions ont été résolues, mais d'autres subsistent. J'espère pouvoir traiter de celles-ci dans mon rapport de l'année prochaine.

On trouvera à l'annexe C la liste de tous les rapports classifiés adressés au ministre par mon prédécesseur et par moi-même depuis l'établissement du bureau du commissaire, en 1996.

Examen des recommandations antérieures

Cette année, mon personnel a passé en revue toutes les recommandations faites par mon prédécesseur et par moi-même dans des rapports classifiés présentés au ministre de la Défense nationale depuis la création de mon bureau, en 1996. Ce travail avait pour but de vérifier la suite donnée à ces recommandations par le CST et de déterminer si les problèmes relevés avaient été réglés de façon satisfaisante. Je demanderai au CST de faire le point annuellement à ce sujet.

Cet examen a révélé que la réponse du CST aux recommandations n'avait pas été uniforme. Cela n'est pas étonnant, compte tenu de la diversité de celles-ci : certaines pouvaient être mises en œuvre immédiatement; certaines avaient trait à la politique ou aux procédures; d'autres étaient de caractère technique, et d'autres encore nécessitaient une étude plus poussée destinée à déterminer leur faisabilité. Beaucoup se rapportaient à la façon dont le CST pourrait mieux gérer ses activités et en rendre compte.

En me fondant sur cet examen, je ferais remarquer que le CST a répondu à beaucoup des recommandations du commissaire, mais qu'il lui reste un certain nombre de questions à aborder, en particulier en établissant des plans de travail et des échéanciers assortis d'étapes et de dates d'achèvement pour les mesures correctives dont il a reconnu la nécessité.

Comme je le dis clairement dans ce rapport, mes recommandations et celles de mon prédécesseur visent généralement à prévenir la possibilité de non-conformité par la mise en place de mécanismes de contrôle efficaces. C'est dans cet esprit que je continuerai à vérifier la suite donnée par le CST aux recommandations de mon bureau.

Constatations faites en 2003-2004

Je puis déclarer que les activités du CST que mon bureau a examinées au cours de la dernière année étaient conformes à la loi et à l'autorisation ministérielle. Il importe de situer cette affirmation dans son contexte. Elle ne signifie pas que je certifie que toutes les activités exercées par le CST en 2003-2004 étaient légales. Je ne peux affirmer cela, car je n'ai pas examiné toutes ses activités — et aucun examinateur indépendant ne pourrait le faire. Toutefois, mon bureau examine un grand nombre d'activités en profondeur, en fonction de notre évaluation des domaines où les risques d'activité illégale sont les plus grands. Tel est le contexte dans lequel il faut envisager la garantie que fournit mon travail.

Je me dois cependant d'ajouter que, au cours des examens, je décèle parfois des circonstances où il existe des risques manifestes d'activité illégale possible (par exemple, en raison de faiblesses dans les politiques ou les pratiques). Tout comme mon prédécesseur, j'ai pour règle de signaler ces circonstances au CST et au ministre. Comme je le déclare clairement dans l'introduction de ce rapport, j'estime qu'il est plus utile de prévenir les activités illégales que de les déceler après le fait.

Plaintes et préoccupations au sujet des activités du CST

Deux plaintes ont été formulées pendant la période couverte par ce rapport, mais ni l'une ni l'autre n'a entraîné une enquête officielle.

Si je dois être en mesure d'assurer aux plaignants que le CST ne se livre pas à des activités illégales, je dois aborder les plaintes en tenant compte du mandat assigné au CST par la partie V.1 de la *Loi sur la défense nationale*. À l'heure actuelle, tout comme avant l'instauration de la partie V.1, le CST ne doit pas cibler les communications de Canadiens ni de personnes se trouvant au Canada. Or, comme je le mentionne plus haut, il n'est désormais plus possible d'affirmer sans équivoque que les deux pôles d'une communication interceptée par le CST sont étrangers. Le CST peut maintenant intercepter (mais non cibler) des communications privées à condition d'obtenir à l'avance une autorisation ministérielle. Il peut aussi utiliser et conserver ces communications à condition de respecter les lignes directrices qui sont également énoncées à la partie V.1 de la *LDN* (voir note 4).

Toutes les plaintes qui me sont présentées au sujet des activités du CST doivent par conséquent être examinées dans cette optique.

Personne ne s'est adressé à moi pour se prévaloir des dispositions relatives à la défense d'intérêt public qui figurent au sous-alinéa 15(5)b)(ii) de la *Loi sur la protection de l'information*[5].

LE BUREAU DU COMMISSAIRE

Dépenses du bureau et personnel

Depuis la création de son poste, en 1996, le mandat du commissaire du Centre de la sécurité des télécommunications et, par conséquent, le personnel et les autres ressources nécessaires à l'exécution de ce mandat ont considérablement évolué. Entre juin 1996 et décembre 2001, le commissaire avait pour rôle d'examiner les activités du CST pour déterminer si elles étaient conformes à la loi, et de recevoir les plaintes relatives à la légalité de ces activités.

[5] L.R.C. (1985), chap. O-5.

Comme les rapports annuels précédents en traitent dans le détail et le présent rapport en fait mention plus haut, deux caractéristiques de la *Loi antiterroriste* de décembre 2001 ont influé directement sur les fonctions du commissaire, soit l'examen des activités entreprises par le CST en vertu d'une autorisation ministérielle, et les fonctions assignées au commissaire en vertu de la *Loi sur la protection de l'information*.

Pour lui permettre de s'acquitter de ces nouvelles responsabilités, on a alloué des ressources additionnelles à mon bureau en vue de l'exécution des travaux d'examen. L'accroissement de la charge de travail et du personnel a influé sur notre façon d'organiser et de gérer notre travail. Par exemple, nous avons amélioré nos politiques et procédures internes de gestion du bureau pour tenir compte du développement de l'organisation et de l'augmentation du personnel au cours de l'année financière.

Nous nous sommes en outre penchés sur nos méthodes de travail. Des outils comme une méthodologie normalisée, des énoncés de portée et des lignes directrices structurent nos examens des activités du CST de sorte que les examinateurs travaillent avec la même rigueur et la même minutie. Comme un plus grand nombre de personnes participent à ces efforts, mon bureau a entrepris de consigner et de décrire ces processus dans tous les cas où c'est possible.

Vu ma nouvelle nomination et l'évolution du mandat du commissaire au cours des trois dernières années, le moment était venu d'examiner les rapports qu'entretient mon bureau dans le contexte plus général où il exerce son activité, notamment avec la collectivité du gouvernement fédéral et la collectivité de la sécurité et du renseignement au Canada et à l'échelle internationale. Un plan de communication élaboré cette année avec le

concours d'acteurs clés de la collectivité canadienne du renseignement aidera à guider mon bureau dans les univers en évolution rapide du renseignement et des politiques.

Par exemple, l'un des objectifs du plan consiste à entretenir des communications plus régulières et plus systématiques avec les groupes et particuliers intéressés — notamment la collectivité canadienne du renseignement, les organismes qui traitent des questions de renseignement et les universitaires spécialisés dans le domaine du renseignement — au sujet de la nature de mon mandat, de ma façon d'aborder mon travail et des activités de mon bureau. Ce genre d'interaction pourrait mener, par exemple, à des partenariats productifs avec des spécialistes des universités dans des domaines d'intérêt et de préoccupation mutuels. De plus, la communication de renseignements exacts et opportuns au sujet de mon bureau aidera à éviter les malentendus ou les conjectures au sujet de sa nature et de ses activités.

Mes rencontres avec le ministre de la Défense nationale actuel et son prédécesseur, avec le président et les membres du Comité de surveillance des activités de renseignement de sécurité et avec le conseiller en matière de sécurité nationale auprès du Premier ministre, dont je fais mention plus haut, ont été parmi les premières mesures d'exécution de ce plan.

De plus, des membres de mon personnel ont rencontré des universitaires spécialisés en matière de sécurité et de renseignement et participé aux réunions de l'Association canadienne pour l'étude de la sécurité et du renseignement. Ils ont également pris des initiatives en vue de participer davantage à la collectivité de la fonction publique, notamment en rencontrant des représentants d'autres petits organismes, en particulier ceux dont le mandat comporte des examens et l'étude de plaintes.

En ce qui concerne la collectivité plus générale de la sécurité et du renseignement, mon bureau a reçu la visite de parlementaires de la Suède et du Royaume-Uni, deux pays qui ont des préoccupations similaires à celles du Canada, mais des modèles d'examen différents. Par le passé, le bureau ne disposait pas d'un personnel suffisant pour se livrer à toutes ces activités, mais le recrutement d'un directeur de l'examen et de la liaison gouvernementale et d'un directeur de l'examen et de la liaison militaire permettra de poursuivre les relations avec ces collectivités à l'avenir.

COUP D'ŒIL SUR L'AVENIR

La nouvelle politique de sécurité nationale

Le 27 avril 2004, le gouvernement a déposé au Parlement sa première politique de sécurité nationale, intitulée *Protéger une société ouverte : la politique canadienne de sécurité nationale*. Celle-ci aborde un grand nombre de questions de sécurité nationale et fournit une orientation dans six domaines stratégiques, soit : le renseignement, la planification et la gestion des opérations d'urgence, la santé publique, la sécurité des transports, la sécurité des frontières, et la sécurité internationale. Elle prévoit en outre l'élaboration de nouvelles structures et stratégies qui, de l'avis du gouvernement, lui permettront de prévoir et de gérer les menaces actuelles et futures pour les intérêts nationaux du Canada en matière de sécurité.

Parmi les modifications de la structure du gouvernement annoncées le 12 décembre 2003 et confirmées lors de l'annonce de la politique de sécurité nationale figurait une proposition visant la constitution d'un nouveau comité de parlementaires dont les membres seraient assermentés à titre de conseillers privés pour pouvoir recevoir des séances d'information sur les questions de sécurité nationale.

Ces initiatives pourraient manifestement influer sur les activités de mon bureau, mais il est trop tôt pour prédire la nature ou l'étendue éventuelles de cette

influence. Mon personnel et moi-même suivrons les événements de près dans le but d'apporter un appoint lorsque ce sera à propos.

Mesures législatives proposées

Deux projets de loi à l'étude au Parlement à la fin de l'année sur laquelle porte le présent rapport pourraient avoir d'autres incidences sur mon bureau :

- le projet de loi C-7 (auparavant projet de loi C-17) est une mesure législative d'ensemble intitulée Loi de 2002 sur la sécurité publique, dont l'adoption entraînerait de nouvelles responsabilités pour le commissaire. Ce projet de loi modifierait la *Loi sur la défense nationale* de manière à attribuer au commissaire du CST de nouvelles responsabilités importantes touchant l'examen de la légalité des mesures prises par le ministère de la Défense nationale et par les Forces canadiennes pour entretenir et protéger leurs systèmes et réseaux informatiques et pour traiter les plaintes découlant de ces mesures[6];
- le projet de loi C-14 (auparavant projet de loi C-32) modifie, entre autres, des dispositions du *Code criminel* et de la Loi sur la gestion des finances publiques. Il instaure de nouvelles dispositions, dont un nouveau pouvoir d'intercepter des communications privées afin de gérer et de protéger les systèmes et réseaux informatiques. On se demande quels effets ce projet de loi aura sur les dispositions et l'adoption du projet de Loi de 2002 sur la sécurité publique, dont le libellé est semblable[7].

---

[6] Projet de loi C-7, *Loi modifiant certaines lois fédérales et édictant des mesures de mise en œuvre de la convention sur les armes biologiques ou à toxines, en vue de renforcer la sécurité publique*, 3e sess., 37e Parl., 2004; projet de loi C-17, *Loi modifiant certaines lois fédérales et édictant des mesures de mise en œuvre de la convention sur les armes biologiques ou à toxines, en vue de renforcer la sécurité publique*, 2e sess., 37e Parl., 2002.

[7] Projet de loi C-14, *Loi modifiant le Code criminel et d'autres lois*, 3e sess., 37e Parl., 2004; projet de loi C-32, *Loi modifiant le Code criminel et d'autres lois*, 2e sess., 37e Parl., 2003.

J'ai trois préoccupations à ce sujet, soit :

- le fait que l'adoption des deux projets de loi établirait des autorisations différentes pour régir des activités essentiellement semblables;
- le fait que l'adoption du projet de loi C-7 imposerait au ministère de la Défense nationale un régime de responsabilisation différent de celui que l'adoption du projet de loi C-14 imposerait aux autres ministères;
- les difficultés auxquelles je me heurterai probablement lorsqu'il s'agira de donner la garantie sérieuse de légalité et de conformité à l'autorisation ministérielle prévue par le projet de loi C-7.

Des faits nouveaux se rattachant à deux autres domaines pourraient également avoir des incidences sur mon bureau :

- l'examen réglementaire de la *Loi antiterroriste* que doit effectuer le Parlement trois ans après son entrée en vigueur doit commencer à la fin de 2004. J'entends apporter mes commentaires en me fondant sur les observations que j'ai faites jusqu'ici;
- le 22 mars 2004, le gouvernement a déposé le projet de loi C-25, ou mesure législative sur la dénonciation[8]. Le CST serait soustrait à cette mesure législative, mais il devrait néanmoins établir un système qui servirait essentiellement à la même fin, ce qui soulève des questions sur un rôle éventuel du commissaire.

Nous suivrons de près ces faits nouveaux et d'autres afin de déterminer leur incidence probable sur mon bureau, ainsi que les domaines où notre apport peut être le plus utile et la façon la plus efficace de le fournir.

---

[8] *Loi prévoyant un mécanisme de dénonciation des actes répréhensibles dans le secteur public et de protection des dénonciateurs*. Son titre abrégé serait : *Loi sur la protection des fonctionnaires dénonciateurs d'actes répréhensibles*, 3e sess., 37e Parl., 2004.

Conférence des organismes d'examen

La prochaine conférence internationale des organismes d'examen des activités de renseignement se tiendra à Washington (D.C.), en octobre 2004. Des représentants des organismes d'examen de l'Australie, du Canada, de la Nouvelle-Zélande, des États-Unis, du Royaume-Uni et d'autres pays se réuniront alors pour échanger des vues sur des questions d'intérêt commun. J'attends de recevoir l'ordre du jour de cette année.

CONCLUSION

Au moment de conclure cette rétrospective, je tiens à remercier mon prédécesseur, l'honorable Claude Bisson, O.C., qui a solidement établi le bureau du commissaire du CST et m'a légué un personnel magnifique et une organisation bien placée pour relever les défis de l'avenir. Grâce à cela, la transition entre son administration et la mienne s'est faite sans heurt, et j'ai pu assumer mes responsabilités rapidement et efficacement.

En me fondant sur mon expérience des neuf derniers mois, j'estime que mon mandat et les ressources mises à ma disposition sont suffisants pour me permettre de m'acquitter des fonctions que me confère la loi. Je compte entretenir les relations productives établies avec le ministre, avec le CST et avec d'autres fonctionnaires tandis que nous remplirons nos rôles respectifs au sein de la collectivité canadienne du renseignement et de la sécurité.

Mandat du commissaire du Centre de la sécurité des télécommunications

Loi sur la défense nationale - Partie V.1

« **273.63** (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

(a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

(b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

(c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

« **273.65** (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre. »

Loi sur la protection de l'information

« **15.** (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public.

« **15.** (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes :

« **15.** (5) (b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession :

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable. »

État des dépenses, 2003-2004

Sommaire des articles courants

Traitements et salaires	352 505
Transports et télécommunications	22 227
Information	43 201
Services professionnels et spéciaux	246 323
Location	134 794
Achat de services de réparation et d'entretien	42 019
Fournitures et approvisionnements	9 708
Acquisition de machines et de matériel	51 451
Autres charges	104
Total	**902 332 $**

Rapports classifiés de 1996 à 2004

Classified Report to the Minister - 3 mars 1997 (TRÈS SECRET)

Classified Report to the Minister
- Operational Policies with Lawfulness Implications - 6 février 1998 - (SECRET)

Classified Report to the Minister
- CSE's activities under *** - 5 mars 1998 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints - 10 mars 1998 (SECRET)

Classified Report to the Minister
- CSE's activities under *** - 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- On controlling communications security (COMSEC) material - 6 mai 1999 (TRÈS SECRET)

Classified Report to the Minister
- How We Test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) - 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- A Study of the *** Collection Program - 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- On *** - 8 décembre 1999 (TRÈS SECRET - COMINT)

Classified Report to the Minister
- A Study of the *** Reporting Process - an overview (Phase I) - 8 décembre 1999 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A Study of Selection and *** - an overview - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's Operational Support Activities Under *** - follow-up - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - 10 mai 2000 (SECRET)

Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - 15 juin 2000 (SECRET)

Classified Report to the Minister
- CSE's Policy System Review - 14 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase II *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase III *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's participation *** - 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's support to ***, as authorized by *** and *** - 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) - 20 août 2002 (SECRET)

Classified Report to the Minister
- CSE's support to XXX as authorized by *** and code named *** - 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's SIGINT activities carried out under the *** 2002 *** ministerial authorization - 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- Lexicon - 26 mars 2003 (TRÈS SECRET/COMINT)

Classified Report to the Minister
- CSE's activities pursuant to three XXX ministerial authorizations including *** *** - 20 mai 2003 (SECRET)

Classified Report to the Minister
- CSE's support to XXX, as authorized by *** and code named *** - Part I - N 6 novembre 2003 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's support to XXX, as authorized by *** and code named *** - Part II - 15 mars 2004 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

Classified Report to the Minister
- A review of CSE's activities conducted under XXX ministerial authorization - 19 mars 2004 (SECRET/Réservé aux canadiens)

Classified Report to the Minister
- Internal investigations and complaints - Follow-up - 25 mars 2004 (TRÈS SECRET/Réservé aux Canadiens)